

PA252-W00
PA253-W06

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-134330

(43) 公開日 平成9年(1997)5月20日

(51) Int.Cl. ^a	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 C
1/00	3 7 0		1/00	3 7 0 E
12/14	3 2 0		12/14	3 2 0 F

審査請求 未請求 請求項の数 7 O L (全 9 頁)

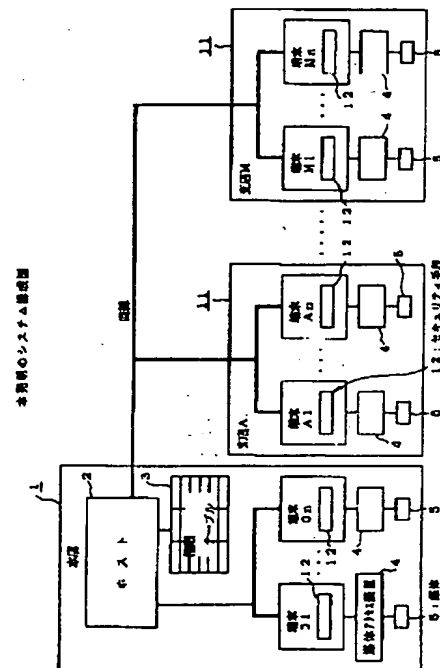
(21) 出願番号	特願平7-289011	(71) 出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(22) 出願日	平成7年(1995)11月7日	(72) 発明者	内海 研二 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72) 発明者	吉岡 誠 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72) 発明者	村上 敬一 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(74) 代理人	弁理士 岡田 守弘

(54) 【発明の名称】 セキュリティ保護システム

(57) 【要約】

【課題】 本発明は、媒体上のデータのセキュリティを保護するセキュリティ保護システムに関し、媒体ID、固有ID、端末IDをチェックしてOKとなったときに暗号化したデータの書き込み/読み出しを許可し、媒体のデータのセキュリティを簡単な処理で実現することを目的とする。

【解決手段】 固有IDを予め書き込んだ媒体と、アクセスしようとする媒体からは固有IDを、端末からは端末毎の端末IDを読み出し、固有IDが正しく、かつ端末IDが正しいときにのみ媒体にアクセス可能とするセキュリティ手段を備えるように構成する。



【特許請求の範囲】

【請求項1】媒体上のデータのセキュリティを保護するセキュリティ保護システムにおいて、固有IDを予め書き込んだ媒体と、アクセスしようとする上記媒体からは固有IDを、端末からは端末毎の端末IDを読み出し、固有IDが正しく、かつ端末IDが正しいときにのみ上記媒体にアクセス可能とするセキュリティ手段を備えたことを特徴とするセキュリティ保護システム。

【請求項2】上記セキュリティ手段は、各端末に備えたことを特徴とする請求項1記載のセキュリティ保護システム。

【請求項3】上記セキュリティ手段は、端末の制御プログラム毎に備えたことを特徴とする請求項1記載のセキュリティ保護システム。

【請求項4】上記固有IDと端末IDにより媒体データの暗号化あるいは復号化を行うことを特徴とする請求項1記載のセキュリティ保護システム。

【請求項5】上記固有ID、端末ID、および利用者IDにより媒体データの暗号化あるいは復号化を行うことを特徴とする請求項1記載のセキュリティ保護システム。

【請求項6】上記固有IDとして、媒体の媒体ID、およびシステム毎に固有な端末IDとしたことを特徴とする請求項1記載のセキュリティ保護システム。

【請求項7】媒体から端末にプログラムをインストールする際に上記セキュリティ手段は、当該媒体に書き込まれている媒体ID、およびインストールしようとする端末の端末IDが正しいときにのみ端末に制御プログラムをインストールすることを特徴とする請求項1記載のセキュリティ保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、媒体上のデータのセキュリティを保護するセキュリティ保護システムに関するものである。

【0002】

【従来の技術】従来、ホストと回線を介して複数の端末が接続されたシステムにおいて、端末にインストールするプログラムや業務処理して結果をMO（光磁気ディスク）などの多量にデータを書き込むことができる媒体に格納し、ホストから端末あるいは端末からホストに運搬することが行われている。この際、データを格納した媒体が紛失したときに他人に盗用されないように運搬を注意して行うようにしていた。

【0003】また、媒体によってはパスワード（識別子）を書き込んでおき、読み出し時にそのパスワード（識別子）を入力しないと読み出せないようにし、媒体が万一紛失しても他人に盗用されないようにしていた。

【0004】

【発明が解決しようとする課題】従来は、上述した前者の端末からホスト、ホストから端末へデータを格納した媒体を注意して運搬していたのでは、万一紛失した場合に他人に盗用されてしまう問題がある。

【0005】また、後者のパスワード（識別子）を媒体に書き込んでおき、読み出した時にパスワード（識別子）を入力しないと読み出せないようにした場合には、パスワード（識別子）が盗用されたときはデータが他人に盗用されてしまう問題がある。

【0006】本発明は、これらの問題を解決するため、媒体ID、固有ID、端末IDをチェックしてOKとなったときに暗号化したデータの書き込み／読み出しを許可し、媒体のデータのセキュリティを簡単な処理で実現することを目的としている。

【0007】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、アクセラ装置4は、媒体5をアクセスするものである。

【0008】セキュリティ手段12は、端末に設け、セキュリティを管理するものである。次に、動作を説明する。固有IDを予め書き込んだ媒体について、セキュリティ手段12がアクセスしようとする媒体からは固有IDを、端末からは端末毎の端末IDを読み出し、固有IDが正しく、かつ端末IDが正しいときにのみ媒体にアクセス可能とするようにしている。

【0009】この際、セキュリティ手段12は、各端末に備えたり、あるいは端末の制御プログラム毎に備えたりするようにしている。また、固有IDと端末IDにより媒体データの暗号化あるいは復号化を行うようにしている。

【0010】また、固有ID、端末ID、および利用者IDにより媒体データの暗号化あるいは復号化を行うようにしている。また、固有IDとして、媒体の媒体ID、およびシステム毎に固有な端末IDとするようにしている。

【0011】また、媒体から端末にプログラムをインストールする際にセキュリティ手段12は、媒体に書き込まれている媒体ID、およびインストールしようとする端末の端末IDが正しいときにのみ端末に制御プログラムをインストールするようにしている。

【0012】従って、媒体5の媒体ID、固有ID、端末IDをチェックしてOKとなったときに暗号化したデータを書き込んだり、読み出したり可能にすることにより、媒体の暗号化されたデータの読出／書込のセキュリティを簡単な処理で実現することが可能となる。

【0013】

【発明の実施の形態】次に、図1から図8を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0014】図1は、本発明のシステム構成図を示す。

図1において、本店1は、各種業務（例えば銀行業務）

を行うものであって、ここでは、ホスト2、権限テーブル3、および複数の端末などから構成されるものである。

【0015】ホスト2は、本店1内の複数の端末、および回線やネットワークを介して接続された支店11内の複数の端末を一括管理するものである。権限テーブル3は、管理者や利用者の権限を管理するものである（図3参照）。

【0016】端末は、ホスト2と通信して業務処理（例えば銀行業務）を行ったり、媒体5にデータを書き込んだり読み出したりなどするものであって、ここでは、セキュリティ手段12および媒体アクセス装置4を備えたものである。

【0017】セキュリティ手段12は、端末が扱うデータなどのセキュリティを管理するものであって、ここでは、媒体アクセス装置4によって媒体5にデータを暗号化して書き込む際のセキュリティなどを管理するものである（後述する）。

【0018】媒体アクセス装置4は、媒体5にデータを読み書きする装置であって、例えばMO（光磁気ディスク装置）や、読み書き可能な光ディスク装置などである。媒体5は、媒体ID、システム固有の固有ID、端末ID、および暗号化されたデータなどを書き込んだり、読みだしたりする可搬媒体である。

【0019】支店11は、本店1のホスト2との間に回線やネットワークを介して接続されたものであって、複数の端末から構成されるものである。以下図1の構成の動作を順次詳細に説明する。

【0020】図2は、本発明の媒体のオーソライズフローチャートを示す。図2において、S1は、一意の媒体IDを書換不可能な領域に書き込む。これは、媒体5である例えばMO（光磁気ディスク）の所定領域にレーザビームで一意の媒体IDを書換不可能な形で書き込む（焼き切る）。これにより、媒体製造メーカが媒体5の出荷時に一意の媒体IDを書換不可能な形で書き込み、媒体5自身の偽造を防止する。

【0021】S2は、管理者のパスワードの入力があるか判別する。これは、図1の本店1の端末の媒体アクセス装置4に、S1で媒体IDを書き込んだ媒体4を挿入したときに、入力されたパスワードが権限テーブル3を参照して管理者のパスワードであるか判別する。YESの場合には、入力されたパスワードが管理者のパスワードであって媒体5を初期化する権限があると判明したので、S3に進む。一方、NOの場合には、入力されたパスワードが管理者のパスワードでなく、媒体5を初期化する権限が無いと判明したので、終了する。

【0022】S3は、S2のYESで初期化する権限ありと判明したので、システム毎の固有IDの決定を行う。これは、システム毎の固有IDとして、例えばA銀行の企業固有IDを決定する。

【0023】S4は、媒体を初期化してオーソライズ媒体を作成する。これは、S3で決定した企業固有IDをS1の媒体5に書き込む。以上によって、後述する図4に示すように、媒体5に、S1で当該媒体出荷時に媒体製造メーカで一意の媒体IDを書換不可能な形で書き込まれ、次に、S4で企業固有IDが書き込まれると共に必要に応じて他の領域（端末ID、暗号化されたデータを格納する領域など）の初期化を行い、当該企業の支店などで使用できる媒体（オーソライズ媒体という）を作成できたこととなる。

【0024】図3は、本発明の権限テーブル例を示す。この権限テーブル3は、図示のようにユーザIDに対応づけて管理者あるいは一般ユーザなどの資格や権限、およびパスワードなどを登録するものである。この権限テーブル3にユーザIDが登録されており、かつ当該ユーザIDに対応づけて登録された資格や権限に対応して業務処理やデータを参照などの権限が決められている。この権限テーブル3を参照して入力されたユーザIDについて管理者の権限があり、かつそのパスワードが入力されたときに、既述した図2のS2のYESとなり、オーソライズ媒体（媒体IDおよび企業固有ID（システム毎に固有な固有ID）を書き込んで初期化した媒体5）を作成できる。

【0025】図4は、本発明のセキュリティ媒体情報例を示す。ここでは、媒体5に図示の下記のセキュリティ媒体情報を書き込む。

- ・媒体ID：出荷時に書き込む、媒体に一意な媒体ID
- ・企業固有ID：企業が本店で媒体初期化として行う（図2のS4）
- ・端末ID：読出／書込許可する端末の固有ID（媒体と端末とをロックする場合に必要であるが、制御プログラムを端末にロックする場合には不要）
- ・暗号化されたデータ
- ・その他

図5は、本発明の特定端末への媒体のロックフローチャートを示す（媒体と端末とをロックする場合に必要であるが、プログラムを端末にロックする場合には不要）。これは、既述した図2のフローチャートに従い、図1の本店1の管理者が媒体製造メーカから書換不可能な形で一意の媒体IDをレーザなどで書き込まれた媒体5に、企業固有IDを更にも書き込むおよび初期化したオーソライズ媒体（図1のS4）について、S11およびS12で特定端末への媒体ロックを行うときのフローチャートである。

【0026】図5において、S11は、端末毎の一意な端末IDを決定する。これは、図1の支店において、管理者が当該支店に設置された各端末に一意な端末IDを決定する。例えば各端末が固有に持つ一意な装置IDを端末IDと決定する。

【0027】S12は、オーソライズ媒体に端末IDを

書き込む。これは、既述した図2のS4で本店で企業固有IDを書き込むおよび初期化したオーソライズ媒体に、S11で決めた端末固有IDを書き込み、媒体が当該端末しか暗号化されたデータを読み書きできないようにいわゆる媒体と端末とをロックする。

【0028】以上によって、本店1から渡されたオーソライズ媒体(図2のS4)について、支店11で更に端末IDを書き込み、媒体5が端末IDの一致する端末しか暗号化されたデータの読み書きができないようにできたこととなる。これにより、媒体5に書き込まれた企業固有IDによって当該企業、更に端末IDによって当該

端末しか暗号化されたデータの読み書きができないようにロックされたこととなる。
【0029】次に、図6のフローチャートに示す順序に従い、後述する図8で特定端末へロックされた制御プログラム(セキュリティ手段12)を用いて、図2で作成されたオーソライズ媒体5に対して、暗号化されたデータを書き込む手順を詳細に説明する。尚、特定端末にロックされた媒体5に対して、暗号化されたデータを書き込むときの手順を括弧内に示す。

【0030】図6は、本発明のデータの書込フローチャートを示す。図6において、S21は、媒体の挿入を行う。これは、暗号化されたデータを媒体5に書き込むとして、当該媒体5をある支店11あるいは本店1のある端末の媒体アクセス装置4に挿入する。

【0031】S22は、媒体IDがあるか判別する。S21で媒体5が媒体アクセス装置4に挿入されたことに対応して、セキュリティ手段12が媒体5の予め定めた所定領域に書き込み不可の形で記録されている媒体IDがあるか判別する。YESの場合には、製造メーカから正規に媒体IDが書き込まれた媒体5と判明したので、S23に進む。NOの場合には、製造メーカから正規に媒体IDが書き込まれた媒体5でないと判明したので、終了する。

【0032】S23は、自企業固有IDがあるか判別する。これは、媒体5の予め定めた所定領域に企業固有IDが書き込まれているか判別する。YESの場合には、本店で企業固有IDが媒体IDに書き込まれた媒体5と判明したので、S24に進む。NOの場合には、企業固有IDが書き込まれた媒体5でないと判明したので、終了する。

【0033】S24は、自端末のアクセス許可があるか判別する。これは、制御プログラム内(あるいは媒体5)に記録されている端末IDと、当該端末IDとが一致してアクセス許可がありか判別する。YESの場合には、アクセス許可有と判明したので、S25に進む。NOの場合には、アクセス許可無と判明したので、終了する。

【0034】S25は、データの暗号化を行う。S26は、データの書込を行う。これらS25およびS26

は、アクセス許可有りと判明したので、データを暗号化(例えば公知のDESなど)して媒体に書き込む。

【0035】以上によって、媒体5上の媒体IDおよび企業固有IDが正しく、かつ制御プログラム内の端末ID(あるいは媒体5上の端末ID)が端末の端末IDと一致したときに、当該制御プログラム(あるいは媒体5)が当該端末に一意にロックされたものと簡単な処理によって判別し、データを暗号化して媒体5に書き込むことが可能となる。

【0036】次に、図7のフローチャートに示す順序に従い、図6で暗号化されたデータの書き込まれた媒体5から暗号化されたデータを読み出す手順を詳細に説明する。図7は、本発明のデータの読出フローチャートを示す。

【0037】図7において、S31は、媒体の挿入を行う。これは、暗号化されたデータを媒体5から読み出そうとして、当該媒体5をある支店11あるいは本店1のある端末の媒体アクセス装置4に挿入する。

【0038】S32は、媒体IDがあるか判別する。S31で媒体5が媒体アクセス装置4に挿入されたことに対応して、セキュリティ手段12が媒体5の予め定めた所定領域に読み書き不可の形で記録されている媒体IDがあるか判別する。YESの場合には、製造メーカから正規に媒体IDが書き込まれた媒体5と判明したので、S33に進む。NOの場合には、製造メーカから正規に媒体IDが書き込まれた媒体5でないと判明したので、終了する。

【0039】S33は、自企業固有IDがあるか判別する。これは、媒体5の予め定めた所定領域に企業固有IDが書き込まれているか判別する。YESの場合には、本店で企業固有IDが媒体IDに書き込まれた媒体5と判明したので、S34に進む。NOの場合には、企業固有IDが書き込まれた媒体5でないと判明したので、終了する。

【0040】S34は、自端末のアクセス許可があるか判別する。これは、制御プログラム内に(あるいは媒体5内に)に記録されている端末IDと、当該端末IDとが一致してアクセス許可がありか判別する。YESの場合には、アクセス許可有と判明したので、S35に進む。NOの場合には、アクセス許可無と判明したので、S35で本店の管理者のパスワードの入力があるか判別し、YESのときには媒体5へのアクセス権がありと判明したのでS36に進み、NOのときには終了する。

【0041】S36は、媒体5から暗号化されたデータの読み出しを行う。S37は、データを復号化する。S38は、データの保存する。

【0042】以上によって、媒体5上の媒体IDおよび企業固有IDが正しく、かつ制御プログラム内の端末ID(あるいは媒体5上の端末ID)が端末の端末IDと一致したときに、当該制御プログラム(あるいは媒体

10

20

30

40

50

5) が当該端末に一意にロックされたものと簡単な処理によって判別し、媒体 5 から暗号化されたデータを読み出して復号化し、保存することが可能となる。

【0043】図 8 は、本発明の制御プログラムのインストールフローチャートを示す。これは、図 1 のセキュリティ手段のプログラム（制御プログラム）を媒体 5 から各端末にインストールし、当該端末でしか制御プログラムを起動できない（あるいは当該媒体 5 を端末にしか再インストールできない）ようにロックし、セキュリティ手段のプログラムが他の端末に無断でインストールされないように防止し、媒体 5 のデータの盗用を防止するためのものである。

【0044】図 8 において、S41 は、プログラムの特定領域に管理者パスワードとシステム毎の固有 ID とを書き込む。S42 は、マスタープログラムをコピーして各支店へ配布する。

【0045】S43 は、各支店の各端末にマスタープログラムをコピーする。S44 は、プログラムの別の特定領域に端末毎の一意な端末 ID を書き込む。これは、支店でマスタープログラムを端末にインストールしてその終わりの状態でマスタープログラムの特定領域に端末 ID を書き込んでマスタープログラムを特定端末に固定し、プログラム起動時にはプログラム内の端末 ID と、インストールした端末の端末 ID とが一致しないとマスタープログラムの起動を禁止するようにするためである（尚、媒体を端末にロックする場合には、マスタープログラムの特定領域に端末 ID を書き込んでマスタープログラムを特定端末に固定し、次回以降のインストール時には、媒体 5 上の端末 ID と、インストールする端末の端末 ID とが一致しないとマスタープログラムの再インストールを禁止するためである）。

【0046】

【発明の効果】以上説明したように、本発明によれば、

媒体 5 の媒体 ID、固有 ID、端末 ID をチェックして OK となったときに暗号化したデータを書き込んだり、読み出したりする構成を採用しているため、媒体の暗号化されたデータの読出／書込のセキュリティを簡単な処理で実現することができる。これらにより、媒体 5 上の一意な媒体 ID、固有 ID、端末 ID のチェックという簡単な処理によって制御プログラム（あるいは媒体 5）が端末にロックされた正当なものの場合のみ媒体 5 のアクセス許可を認め、それ以外はアクセス禁止として媒体が万一他人に渡っても暗号化されたデータの読み出しを不可とし、次に処理に時間のかかるデータを暗号化して書き込んだり、読み出した暗号化されたデータを復号したりし、セキュリティの完全を期することが可能となる。

【図面の簡単な説明】

【図 1】本発明のシステム構成図である。

【図 2】本発明の媒体のオーソライズフローチャートである。

【図 3】本発明の権限テーブル例である。

【図 4】本発明のセキュリティ媒体情報例である。

【図 5】本発明の特定端末への媒体のロックフローチャートである。

【図 6】本発明のデータの書込フローチャートである。

【図 7】本発明のデータの読出フローチャートである。

【図 8】本発明の制御プログラムのインストールフローチャートである。

【符号の説明】

- 1：本店
- 2：ホスト
- 3：権限テーブル
- 4：媒体アクセス装置
- 5：媒体
- 11：支店
- 12：セキュリティ手段

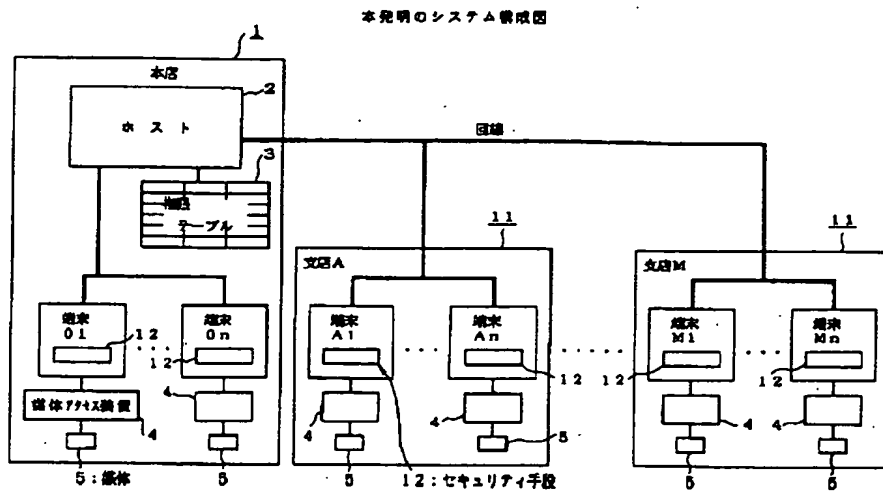
【図 3】

本発明の権限テーブル例

3

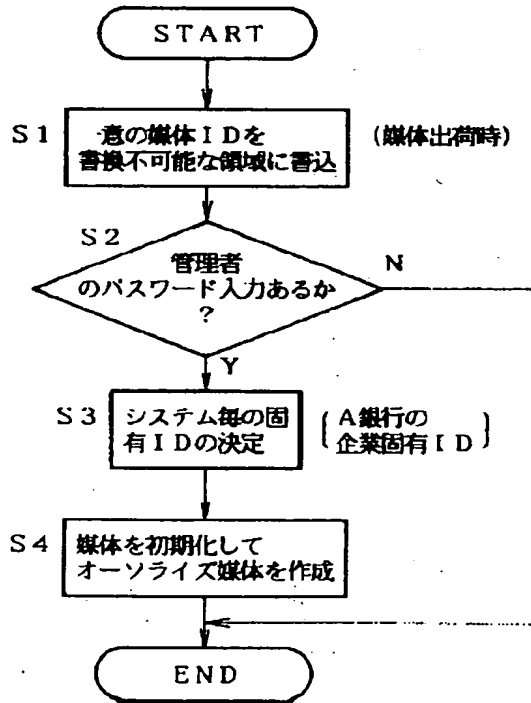
ユーザ ID	資格（権限）	パスワード	
xxx	管理者／ 般ユーザ	xxxxx	

【図1】



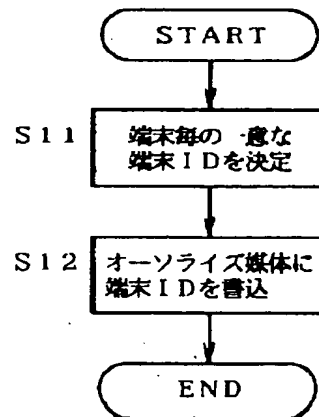
【図2】

本発明の媒体のオーソライズフローチャート



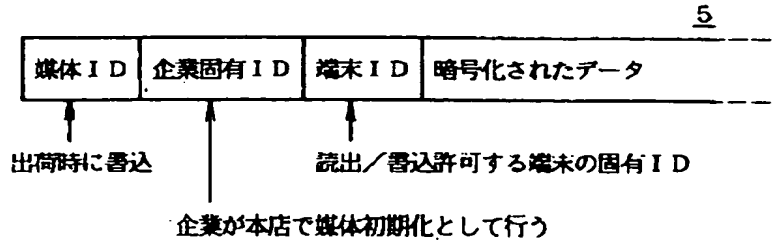
【図5】

本発明の特定端末への媒体のロックフローチャート



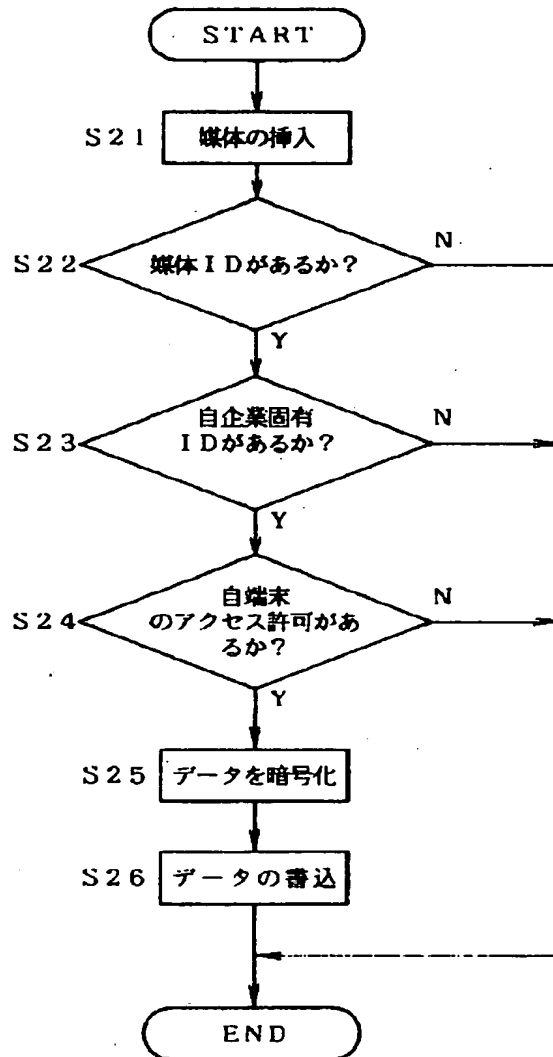
【図4】

本発明のセキュリティ媒体情報例

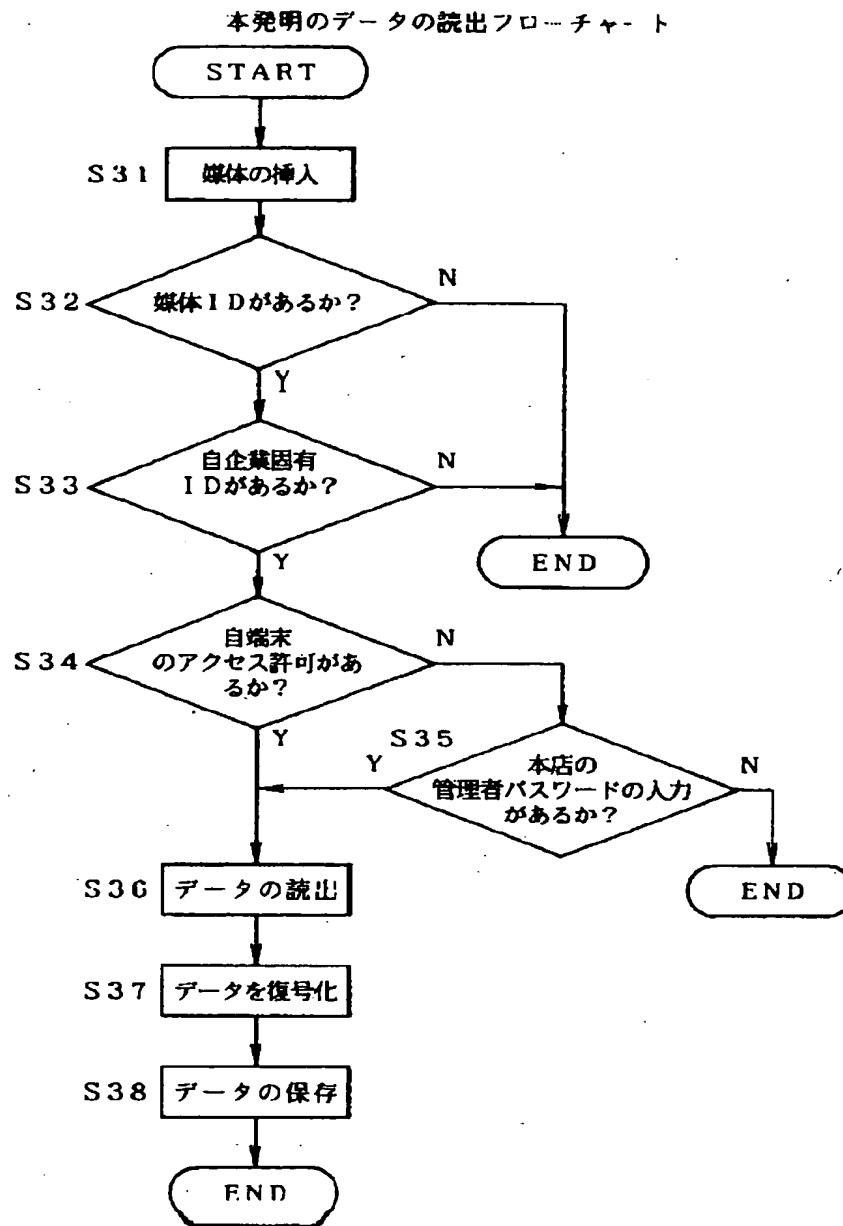


【図6】

本発明のデータ書込フローチャート



【図7】



【図8】

本発明の制御プログラムのインストールフローチャート

